FIPS 140-2 Security Policy

BlackBerry Enterprise Server Cryptographic Kernel Version 1.0.2.5

Document Version 1.4

Government Certifications Team

Research In Motion

Document and Contact Information

Version	Date	Author	Description
1.0	21 June 2005	David MacFarlane	Document creation.
1.1	27 June 2005	David MacFarlane	Updated to module version 1.0.2.5.
1.2	13 July 2005	David MacFarlane	Updated during conformance testing.
1.3	19 July 2005	David MacFarlane	Algorithm certificate information updated.
1.4	27 October 2005	David MacFarlane	Corrected AES information and updated per CMVP feedback.

Contact	Corporate Office
Government Certifications Team certifications@rim.com (519) 888-7465 ext. 2921	**Research In Motion** 295 Phillip Street Waterloo, Ontario Canada N2L 3W8 www.rim.com www.blackberry.com

Contents

List of Tables

List of Figures

Introduction

BlackBerry® is the leading wireless solution that allows users to stay connected to a full suite of applications, including email, phone, enterprise applications, Internet, Short Messaging Service (SMS), and organiser information. BlackBerry is a totally integrated package that includes innovative software, advanced BlackBerry Wireless Handhelds™ and wireless network service, providing a seamless solution. The BlackBerry architecture is shown in the following figure.

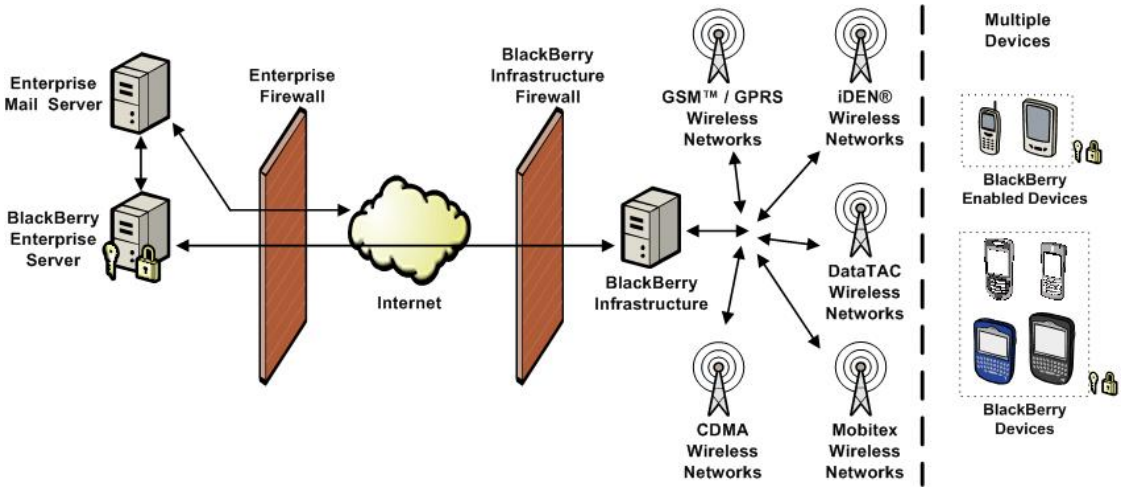

Figure 1. BlackBerry Solution Architecture

BlackBerry Enterprise Server™ software tightly integrates with Microsoft® Exchange, IBM® Lotus® Domino®, and Novell® GroupWise® while working with other existing enterprise systems to enable push-based access of wireless email and data. It allows users to securely send and receive email and information from enterprise data stores and applications. BlackBerry Enterprise Server provides simplified management and centralised control of the wireless environment with industry-standard performance monitoring capabilities, administrative tools, and wirelessly-enabled IT policies. BlackBerry Enterprise Server also enables several other productivity enhancements, including attachment viewing for popular file formats, wireless calendar synchronisation, and remote address lookup.

BlackBerry Enterprise Server provides simplified management and centralised control of the wireless environment with industry-standard performance monitoring capabilities, administrative tools and wirelessly-enabled IT policies. It also allows IT departments to benefit from a scalable and flexible solution that meets their evolving wireless requirements. For more information on the BlackBerry solution, visit http://www.blackberry.com/.

The BlackBerry Enterprise Server Cryptographic Kernel, hereafter referred to as *cryptographic module* or *module*, is a software cryptographic module that provides the following cryptographic services to the BlackBerry Enterprise Server:

- Data encryption and decryption
- Message digest and authentication code generation
- Random data generation
- Elliptic curve key pair generation
- Elliptic curve digital signature generation and verification
- Elliptic curve key agreement

Cryptographic Module Specification

Security Functions

The cryptographic module is a software module in the form of a dynamically linked library (DLL) file that implements the following FIPS-Approved security functions[1]:

- **AES-128**, **-192**, and **-256** (encrypt and decrypt), as specified in FIPS 197. The implementation supports the ECB and CBC modes of operation and has been awarded certificate no. 289 on the AES Validation List, http://csrc.nist.gov/cryptval/aes/aesval.html.
- **Triple DES** (encrypt and decrypt), as specified in FIPS 46-3. The implementation supports the ECB and CBC modes of operation and has been awarded certificate no. 364 on the Triple DES Validation List, http://csrc.nist.gov/cryptval/des/tripledesval.html.
- **SHA-1**, **-224**, **-256**, **-384**, and **-512**, as specified in FIPS 180-2. The implementation has been awarded certificate no. 363 on the SHS Validation List, http://csrc.nist.gov/cryptval/shs/shaval.htm.
- **HMAC SHA-1**, **-224**, **-256**, **-384**, and **-512**, as specified in FIPS 198. The implementation has been awarded certificate no. 98 on the HMAC Validation List, http://csrc.nist.gov/cryptval/mac/hmacval.html.
- **FIPS 186-2 RNG**, as specified in FIPS 186-2. The implementation has been awarded certificate no. 114 on the RNG Validation List, http://csrc.nist.gov/cryptval/rng/rngval.html.
- **ECDSA**, as specified in FIPS 186-2 and ANSI X9.62. The implementation supports elliptic curves P-521 and K-571 and has been awarded certificate no. 8 on the ECDSA Validation List, http://csrc.nist.gov/cryptval/dss/ecdsaval.html.

The module implements the following non-Approved security functions:

- **EC Diffie-Hellman** (key agreement, key establishment methodology provides 256 bits of encryption strength), as specified in IEEE P1363 Draft 13. Per *FIPS 140-2 Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2*, the implementation may presently be used in a FIPS-Approved mode of operation. The implementation supports elliptic curves P-521 and K-571.
- **ECMQV** (key agreement, key establishment methodology provides 256 bits of encryption strength), as specified in IEEE P1363 Draft 13. Per *FIPS 140-2 Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2*, the implementation may presently be used in a FIPS-Approved mode of operation. The implementation supports elliptic curves P-521 and K-571.
- **Rijndael**. The implementation supports the ECB and CBC modes of operation; key lengths of 128, 160, 192, 224, and 256 bits; and block lengths of 128[2], 160, 192, 224, and 256 bits.

Cryptographic Boundary

The physical boundary of the module is the physical boundary of the general purpose computer (GPC) that executes the module and is shown in the following figure.

[1] A security function is FIPS-Approved if it is explicitly listed in *FIPS 140-2 Annex A: Approved Security Functions for FIPS PUB 140-2*.
[2] Supported for key lengths of 160 and 224 bits only.

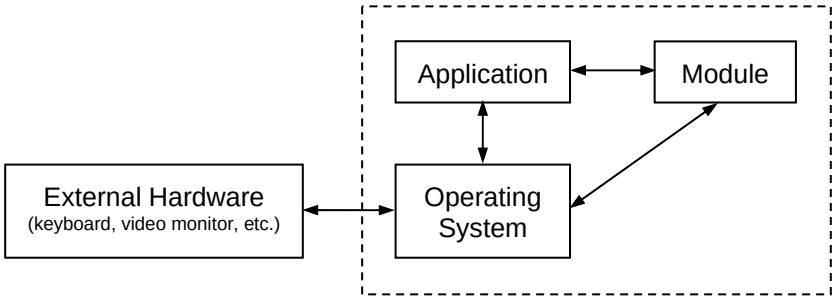

Figure 2. Physical Boundary

Determining the Module Version

The operator may determine the version of the module by viewing the properties screen on the DLL file:

1. Navigate to and right-click on the module file, i.e. CE.dll.
2. Select **Properties** from the resulting context menu.
3. Select the Version tab.
4. The versioning information screen appears and displays the module version, e.g. “1.0.2.5”.

Cryptographic Module Ports and Interfaces

The physical ports of the module correspond to the ports of the GPC that executes the module, and the logical interface of the module is its application programming interface (API). The module implements the FIPS 140-2 interfaces as described in the following table.

Table 1. Implementation of FIPS 140-2 Interfaces

FIPS 140-2 Interface	Module Ports	Module Interfaces
Data Input	GPC input ports (e.g. keyboard, mouse)	Input parameters of API function calls
Data Output	GPC output ports (e.g. video display)	Output parameters of API function calls
Control Input	GPC control input ports (e.g. keyboard, power switch)	API function calls
Status Output	GPC status output ports (e.g. video display, LED)	Function calls that return status information and return code provided by each API function call
Power Input	GPC power input ports (e.g. power supply)	Not supported
Maintenance	GPC maintenance port (e.g. access panel)	Not supported

Roles, Services, and Authentication

Roles

The module supports a User and Crypto Officer role. The module does not support a maintenance role, nor does it support concurrent operators.

Services

The services described in the following table are available to the operator.

Table 2. Module Services

Service	Description
Show Status	Displays the status of the module.
Perform Self-Tests	If invoked via the SelfTest function call, executes the cryptographic algorithm known answer tests. If invoked by powering on the module, executes the power-up self-tests.
Encrypt Data	Encrypts data using AES, Triple DES, or Rijndael, as specified by the operator.
Decrypt Data	Decrypts data using AES, Triple DES, or Rijndael, as specified by the operator.
Create Message Digest	Calculates a message digest using SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512, as specified by the operator.
Create MAC	Calculates a message authentication code using HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, or HMAC SHA-512, as specified by the operator.
Generate Random Data	Generates random data using the FIPS 186-2 RNG.
Generate Key Pair	Generates an elliptic curve key pair, consisting of a public and private key.
Generate Signature	Generates a digital signature using ECDSA.
Verify Signature	Verifies an ECDSA digital signature.
Perform Key Agreement	Cooperatively calculates a symmetric key with another party through elliptic curve Diffie-Hellman or elliptic curve MQV key agreement.

Authentication

The module does not support operator authentication. Roles are implicitly selected based on the service performed by the operator. Implicit role selection is summarised in the following table, as are the keys and critical security parameters (CSPs) that are affected by each service.

Table 3. Role Selection by Module Service

Service	Role Implicitly Selected	Affected Keys and CSPs	Access to Keys and CSPs
Show Status	User	N/A	N/A
Perform Self-Tests	Crypto Officer	Software Integrity Key	Execute
Encrypt Data	User	AES Key Triple DES Key Rijndael Key	Execute
Decrypt Data	User	AES Key Triple DES Key Rijndael Key	Execute
Create Message Digest	User	N/A	N/A
Create MAC	User	HMAC Key	Execute

Service	Role Implicitly Selected	Affected Keys and CSPs	Access to Keys and CSPs
Generate Random Data	User	N/A	N/A
Generate Key Pair	User	ECC Key Pair	Write
Generate Signature	User	ECC Private Key	Execute
Verify Signature	User	ECC Public Key	Execute
Perform Key Agreement	User	ECC Key Pair	Execute
		AES Key Triple DES Key Rijndael Key	Write

Physical Security

The module is implemented entirely in software, thus the FIPS 140-2 physical security requirements are not applicable.

Operational Environment

The module is designed to execute on a GPC in conjunction with the BlackBerry Enterprise Server application. The minimum requirements for the operational environment of the BlackBerry Enterprise Server application are listed in the following table, based on the enterprise messaging environment.

Table 4. BlackBerry Enterprise Server Operational Environments

Messaging Environment	Minimum Operational Environment
Microsoft Exchange	• Microsoft Windows® 2000 Server; or • Microsoft Windows 2000 Advanced Server; or • Microsoft Windows Server™ 2003
IBM Lotus Domino	• Microsoft Windows 2000 Server; or • Microsoft Windows 2000 Advanced Server; or • Microsoft Windows Server 2003
Novell GroupWise	• Microsoft Windows 2000 Server Service Pack 4; or • Microsoft Windows 2000 Advanced Server Service Pack 4; or • Microsoft Windows Servers 2003

The operating system is restricted to a single user mode of operation per FIPS 140-2 Implementation Guidance 6.1, i.e. the BlackBerry Enterprise Server application is the single user of the module, even when the server application is serving multiple clients.

For the purposes of FIPS 140-2 conformance testing, the module was tested on Windows 2000 Server SP 4, however the module may be executed on any of the supported operating systems and remain FIPS-compliant.

Cryptographic Keys and Critical Security Parameters

The following table describes the cryptographic keys, key components, and CSPs utilised by the module.

Table 5. Cryptographic Keys and CSPs

Key / CSP	Description
AES Key	A symmetric key used to encrypt and decrypt data using the AES algorithm. The module supports AES key lengths of 128, 192, and 256 bits.
Triple DES Key	A symmetric key used to encrypt and decrypt data using the Triple DES algorithm. Per the specification of Triple DES, all Triple DES keys are 192 bits in length.
HMAC Key	A key used to calculate a message authentication code using the HMAC algorithm. The length of the HMAC key is dependent on the underlying hash algorithm.
Software Integrity Key	A 128-bit HMAC SHA-1 key used to verify the integrity of the module.
ECC Key Pair	A key pair used to generate and verify digital signatures or to perform key agreement over elliptic curves.
Rijndael Key	A symmetric key used to encrypt and decrypt data using the Rijndael algorithm. The module supports Rijndael key lengths of 160 and 224 bits.

Self-Tests

The module implements the self-tests described in the following table.

Table 6. Module Self-Tests

Test	Description
Software Integrity Test	The Software Integrity Test verifies the integrity of the module software using HMAC SHA-1.
FIPS 186-2 RNG Known Answer Test	The FIPS 186-2 RNG known answer test (KAT) verifies that the RNG is operating correctly.
AES Known Answer Test	The AES KAT verifies that the AES encryption and decryption functions are operating correctly.
Triple DES Known Answer Test	The Triple DES KAT verifies that the Triple DES encryption and decryption functions are operating correctly.
SHA-1 Known Answer Test	The SHA-1 KAT verifies that the SHA-1 hashing function is operating correctly.
SHA-224 Known Answer Test	The SHA-224 KAT verifies that the SHA-224 hashing function is operating correctly.
SHA-256 Known Answer Test	The SHA-256 KAT verifies that the SHA-256 hashing function is operating correctly.
SHA-384 Known Answer Test	The SHA-384 KAT verifies that the SHA-384 hashing function is operating correctly.
SHA-512 Known Answer Test	The SHA-512 KAT verifies that the SHA-512 hashing function is operating correctly.
HMAC SHA-1 Known Answer Test	The HMAC SHA-1 KAT verifies that the HMAC SHA-1 function is operating correctly.
HMAC SHA-224 Known Answer Test	The HMAC SHA-224 KAT verifies that the HMAC SHA-224 function is operating correctly.
HMAC SHA-256 Known Answer Test	The HMAC SHA-256 KAT verifies that the HMAC SHA-256 function is operating correctly.
HMAC SHA-384 Known Answer Test	The HMAC SHA384 KAT verifies that the HMAC SHA-384 function is operating correctly.
HMAC SHA-512 Known Answer Test	The HMAC SHA-512 KAT verifies that the HMAC SHA-512 function is operating correctly.
Continuous RNG Test	The module implements a continuous RNG test, as specified in FIPS 140-2, for the implemented FIPS 186-2 RNG.
ECC Pair-Wise Consistency Test	The module executes a pair-wise consistency test for each newly created ECC key pair.
ECDSA Pair-Wise Consistency Test	The ECDSA pair-wise consistency test verifies that the ECDSA signature creation and verification functions are operating correctly.

When an operator attempts to load the module into GPC memory, the power-up self-tests are executed. The power-up self-tests comprise of all the tests identified above with the exception of the Continuous RNG Test and the ECC Pair-Wise Consistency Test. The Software Integrity Test is the first self-test executed, and if it fails then the attempt to load the module fails. If a cryptographic algorithm KAT fails then the operator may not access the corresponding algorithm until the KAT is executed successfully.

The operator may invoke the power-up self-tests by unloading and reloading the module into GPC memory. The operator may also invoke all of the power-up self-tests, except the Software Integrity Test, by invoking the **Perform Self-Tests** service.

Mitigation of Other Attacks

The module is not designed to mitigate any specialised attacks, thus the FIPS 140-2 requirements for mitigation of other attacks are not applicable.

Installation and Start-Up

The module is installed as part of the BlackBerry Enterprise Server application, thus there are no module-specific installation instructions. The installation instructions for the BlackBerry Enterprise Server application for the appropriate messaging environment should be followed and are given in the following documents, available from http://www.blackberry.com/:

- *BlackBerry Enterprise Server for IBM Lotus Domino Installation Guide*
- *BlackBerry Enterprise Server for Microsoft Exchange Installation Guide*
- *BlackBerry Enterprise Server for Novell GroupWise Installation Guide*

FIPS 140-2 Mode of Operation

In order to operate the module in a FIPS-Approved manner, the following conditions must be met:

1. The Rijndael algorithm is not used for data encryption or decryption. More specifically, the following input parameters are not used in any of the AES API function calls:
   - Keys that are 160 or 224 bits in length
   - Keys that are 128, 192, or 256 bits in length when a block size of 160, 192, 224, or 256 bits is specified.

Glossary

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application programming interface
CBC	Cipher block chaining
CSP	Critical security parameter
DES	Data Encryption Standard
EC	Elliptic curve
ECB	Electronic code book
ECC	Elliptic curve cryptography
ECDSA	Elliptic curve Digital Signature Algorithm
ECMQV	Elliptic curve Menezes, Qu, Vanstone
FIPS	Federal Information Processing Standard
GPC	General purpose computer
HMAC	Keyed-hashed message authentication code
IEEE	Institute of Electrical and Electronics Engineers
KAT	Known answer test
MAC	Message authentication code
PUB	Publication
RIM	Research In Motion
RNG	Random number generator
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMS	Short Messaging Service